

# Quantum hypothesis testing and sufficient subalgebras

Anna Jenčová\*

Mathematical Institute, Slovak Academy of Sciences  
Štefánikova 49, 814 73 Bratislava, Slovakia

We introduce a new notion of a sufficient subalgebra for quantum states: a subalgebra is 2- sufficient for a pair of states  $\{\rho_0, \rho_1\}$  if it contains all Bayes optimal tests of  $\rho_0$  against  $\rho_1$ . In classical statistics, this corresponds to the usual definition of sufficiency. We show this correspondence in the quantum setting for some special cases. Furthermore, we show that sufficiency is equivalent to 2 - sufficiency, if the latter is required for  $\{\rho_0^{\otimes n}, \rho_1^{\otimes n}\}$ , for all  $n$ .

MSC: 46L53, 81R15, 62B05.

*Key words:* quantum hypothesis testing, sufficient subalgebras, 2-sufficiency, quantum Chernoff bound

## 1 Introduction

In order to motivate our results, let us consider the following problem of classical statistics. Suppose that  $P_0$  and  $P_1$  are two probability distributions and the task is to discriminate between them by an  $n$ -dimensional observation vector  $X$ . The problem is, if there is a function (statistic)  $T : X \rightarrow Y$ , such that the vector  $Y = T(X)$  (usually of lower dimension) contains all information needed for the discrimination.

---

\*Email: jenca@mat.savba.sk. Supported by the Slovak Research and Development Agency under the contract No. APVV 0071-06, grant VEGA 2/0032/09, Center of Excellence SAS - Quantum Technologies and ERDF OP R&D Project CE QUTE ITMS 26240120009

In the setting of hypothesis testing, the null hypothesis  $H_0 = P_0$  is tested against the alternative  $H_1 = P_1$ . In the most general formulation, a test is a measurable function  $\varphi : X \rightarrow [0, 1]$ , which can be interpreted as the probability of rejecting the hypothesis if  $x \in X$  occurs. There are two kinds of errors appearing in hypothesis testing: it may happen that  $H_0$  is rejected, although it is true (error of the first kind), or that it is not rejected when  $H_1$  is true (error of the second kind). For a given test  $\varphi$ , the error probabilities are

$$\begin{aligned}\alpha(\varphi) &= \int \varphi(x) P_0(dx) && \text{first kind} \\ \beta(\varphi) &= \int (1 - \varphi(x)) P_1(dx) && \text{second kind}\end{aligned}$$

The two kinds of errors are in some sense complementary and it is usually not possible to minimize both error probabilities simultaneously. In the Bayesian approach, we choose a prior probability distribution  $\{\lambda, 1 - \lambda\}$ ,  $\lambda \in [0, 1]$  on the two hypotheses and then minimize the average (Bayes) error probability

$$\int \varphi(x) \lambda P_0(dx) + \int (1 - \varphi(x)) (1 - \lambda) P_1(dx) = \lambda \alpha(\varphi) + (1 - \lambda) \beta(\varphi).$$

Suppose now that  $T$  is a sufficient statistic for  $\{P_0, P_1\}$ . Roughly speaking, this means that there exists a common version of the conditional expectation  $E[\cdot|T] = E_{P_0}[\cdot|T]$ ,  $P_0$ - a.s. and  $E[\cdot|T] = E_{P_1}[\cdot|T]$ ,  $P_1$ - a.s. If  $\varphi$  is any test, then  $E[\varphi|T]$  is another test having the same error probabilities. It follows that we can always have an optimal test that is a function of  $T$ , so that only values of  $T(X)$  are needed for optimal discrimination between  $P_0$  and  $P_1$ .

The following theorem states that this can happen if and only if  $T$  is sufficient, so that the above property characterizes sufficient statistics. The theorem was proved by Pfanzagl, see also [16].

**Theorem 1** [15] *Let  $T : X \rightarrow Y$  be a statistic. The following are equivalent.*

1. *For any  $\lambda \in (0, 1)$  and any test  $\varphi : X \rightarrow [0, 1]$ , there exists a test  $\psi : Y \rightarrow [0, 1]$ , such that*

$$\lambda \alpha(\psi \circ T) + (1 - \lambda) \beta(\psi \circ T) \leq \lambda \alpha(\varphi) + (1 - \lambda) \beta(\varphi)$$

2.  *$T$  is a sufficient statistic for  $\{P_0, P_1\}$ .*

The problem of hypothesis testing can be considered also in the quantum setting. Here we deal with a pair of density operators  $\rho_0, \rho_1 \in B(\mathcal{H})$ , where  $\mathcal{H}$  is a finite dimensional Hilbert space and all tests are given by operators  $0 \leq M \leq 1$ ,  $M \in B(\mathcal{H})$ . The problem of finding the optimal tests (the quantum Neyman-Pearson tests) and average error probabilities was solved by Helstrom and Holevo [6, 8].

Here a question arises, if it is possible to discriminate the states optimally by measuring on a given subsystem. Then we can gain some information only on the restricted densities, which, in general, can be distinguished with less precision.

Let  $M_0 \subseteq B(\mathcal{H})$  be the subalgebra describing the subsystem we have access to. The average error probabilities for tests in  $M_0$  are usually higher than the optimal ones. We will consider the situation that this does not happen and  $M_0$  contains some optimal tests for all prior probabilities. In agreement with classical terminology (see [16]), such a subalgebra will be called sufficient with respect to testing problems, or 2-sufficient, for  $\{\rho_0, \rho_1\}$ .

The quantum counterpart of sufficiency was introduced and studied by Petz, see Chap. 9. in [13], in a more general context. According to this definition, the subalgebra  $M_0$  is sufficient for  $\{\rho_0, \rho_1\}$ , if there exists a completely positive, trace preserving map  $M_0 \rightarrow B(\mathcal{H})$ , that maps both restricted densities to the original ones. Then the restriction to  $M_0$  preserves all information needed for discrimination between the states and it is quite easy to see that a sufficient subalgebra must be 2-sufficient.

The conditions for sufficiency seem to be quite restrictive (see for example the factorization conditions in [9]) and might be too strong, if only hypothesis testing is considered. It is therefore natural to ask if there is a quantum version of Theorem 1, that is, if every 2-sufficient subalgebra must be sufficient.

In this paper, we give a partial answer to this question. We show that 2-sufficiency and sufficiency are equivalent under each of the following conditions: 1) the subalgebra  $M_0$  is invariant under the modular group of one of the states, 2)  $M_0$  is commutative, 3)  $\rho_0$  and  $\rho_1$  commute. Moreover, we show that if the 2-sufficiency condition is strengthened to hold for  $n$  independent copies of the densities for all  $n$ , then the two notions become equivalent.

The organization of the paper is as follows. In Section 2, some basic notions are introduced and several characterizations of a sufficient subalgebra are given. A new characterization, based on a version of the Radon-Nikodym derivative, is found, this will be needed for the main results. Section 3 gives the quantum Neyman-Pearson lemma and quantum Chernoff bound. Section 4 contains the main results: a convenient necessary condition for 2-sufficiency is found and it is shown that it implies sufficiency in the three above described

cases. Finally, the quantum Chernoff bound is utilized to treat the case when 2-sufficiency holds for  $n$  independent copies of the states, for all  $n$ .

## 2 Some basic definitions and facts

### 2.1 Generalized conditional expectation

Let  $\mathcal{H}$  be a finite dimensional Hilbert space and let  $\rho$  be an invertible density matrix. Let  $M_0 \subseteq B(\mathcal{H})$  be a subalgebra and let  $E : B(\mathcal{H}) \rightarrow M_0$  be the trace preserving conditional expectation. Then  $E(\rho)$  is the restricted density of the state  $\rho$ .

As we have seen, the classical sufficient statistic is defined by certain property of the conditional expectations. It is well known that in the quantum case, a state preserving conditional expectation does not always exist. Therefore we need the generalized conditional expectation, defined by Accardi and Cecchini [1]. In our setting, it can be given as follows.

Let us introduce the inner product  $\langle X, Y \rangle_\rho = \text{Tr } X^* \rho^{1/2} Y \rho^{1/2}$  in  $B(\mathcal{H})$ . Then the generalized conditional expectation  $E_\rho$  is a map  $B(\mathcal{H}) \rightarrow M_0$ , defined by

$$\langle X_0, Y \rangle_\rho = \langle X_0, E_\rho(Y) \rangle_{E(\rho)}, \quad X_0 \in M_0, Y \in B(\mathcal{H})$$

It is easy to see that we have

$$E_\rho(X) = E(\rho)^{-1/2} E(\rho^{1/2} X \rho^{1/2}) E(\rho)^{-1/2} \quad (1)$$

It is known that  $E_\rho$  is completely positive and unital and that it is a conditional expectation if and only if  $\rho^{it} M_0 \rho^{-it} \subseteq M_0$ , for all  $t \in \mathbb{R}$ . It is also easy to see that  $E_\rho$  preserves the state  $\rho$ , that is,  $E_\rho^* \circ E(\rho) = \rho$ .

Next we introduce two subalgebras, related to  $E_\rho$ . Let  $F_\rho$  be the set of fixed points of  $E_\rho$  and let  $N_\rho \subseteq B(\mathcal{H})$  be the multiplicative domain of  $E_\rho$ ,

$$N_\rho = \{X \in B(\mathcal{H}), E_\rho(X^* X) = E_\rho(X)^* E_\rho(X), E_\rho(X X^*) = E_\rho(X) E_\rho(X)^*\}$$

Then both  $F_\rho$  and  $N_\rho$  are subalgebras in  $B(\mathcal{H})$ . It is clear that  $F_\rho \subseteq M_0 \cap N_\rho$ , moreover,  $X \in F_\rho$  if and only if  $\rho^{it} X \rho^{-it} \in M_0$  for all  $t \in \mathbb{R}$ . As for  $N_\rho$ , we have the following result.

**Lemma 1**  $N_\rho = \rho^{1/2} M_0 \rho^{-1/2} \cap \rho^{-1/2} M_0 \rho^{1/2}$

*Proof.* It is clear from (1) that  $X \in N_\rho$  if and only if

$$\begin{aligned} E(\rho^{1/2} X^* X \rho^{1/2}) &= E(\rho^{1/2} X^* \rho^{1/2}) E(\rho)^{-1} E(\rho^{1/2} X \rho^{1/2}) \\ E(\rho^{1/2} X X^* \rho^{1/2}) &= E(\rho^{1/2} X \rho^{1/2}) E(\rho)^{-1} E(\rho^{1/2} X^* \rho^{1/2}) \end{aligned}$$

Let  $A = X\rho^{1/2}$ ,  $B = \rho^{1/2}$ . Similarly as in [11], we put  $M = A - B\Lambda$ , with  $\Lambda = E(\rho)^{-1}E(\rho^{1/2}X\rho^{1/2})$ . Then from  $E(M^*M) \geq 0$ , we obtain

$$E(A^*A) \geq E(A^*B)E(\rho)^{-1}E(B^*A),$$

with equality if and only if  $M = 0$ , this implies

$$\rho^{-1/2}X\rho^{1/2} = E(\rho)^{-1}E(\rho^{1/2}X\rho^{1/2}) \in M_0.$$

Conversely, let  $X_0 = \rho^{-1/2}X\rho^{1/2} \in M_0$ , then  $E(\rho^{1/2}X\rho^{1/2}) = E(\rho)X_0$ , this implies that  $M = 0$ .

Similarly, we get that  $\rho^{-1/2}X^*\rho^{1/2} \in M_0$  is equivalent with the second equality. □

It is also known that  $E_\rho(XY) = E_\rho(X)E_\rho(Y)$ ,  $E_\rho(YX) = E_\rho(Y)E_\rho(X)$  for all  $X \in N_\rho$ ,  $Y \in B(\mathcal{H})$ , this can be also shown from the above Lemma. Note that in the case that  $E_\rho$  is a conditional expectation,  $F_\rho = N_\rho = M_0$ .

## 2.2 A Radon-Nikodym derivative and relative entropies

Let  $\rho_0, \rho_1$  be invertible density matrices in  $B(\mathcal{H})$ . We will use the quantum version of the Radon-Nikodym derivative introduced in [5]. In our setting, the derivative  $d_{\rho_0, \rho_1}$  of  $\rho_1$  with respect to  $\rho_0$  is defined as the unique element in  $B(\mathcal{H})$ , such that  $\text{Tr } \rho_1 X = \langle X^*, d_{\rho_0, \rho_1} \rangle_{\rho_0}$ . Then clearly

$$d_{\rho_0, \rho_1} = \rho_0^{-1/2} \rho_1 \rho_0^{-1/2}$$

so that  $d_{\rho_0, \rho_1}$  is positive, and  $\|d_{\rho_0, \rho_1}\| \leq \lambda$  for any  $\lambda > 0$ , such that  $\rho_1 \leq \lambda \rho_0$ . It is also easy to see that

$$E_{\rho_0}(d_{\rho_0, \rho_1}) = d_{E(\rho_0), E(\rho_1)}$$

Let us recall that the Belavkin - Staszewski relative entropy is defined as [5]

$$S_{BS}(\rho_1, \rho_0) = -\text{Tr } \rho_0 \eta(\rho_0^{-1/2} \rho_1 \rho_0^{-1/2}) = -\text{Tr } \rho_0 \eta(d_{\rho_0, \rho_1})$$

where  $\eta(x) = -x \log(x)$ . Let  $S$  be the Umegaki relative entropy

$$S(\rho_1, \rho_0) = \text{Tr } \rho_1 (\log \rho_1 - \log \rho_0)$$

then  $S(\rho_1, \rho_0) \leq S_{BS}(\rho_1, \rho_0)$ , [7] and  $S(\rho_1, \rho_0) = S_{BS}(\rho_1, \rho_0)$  if  $\rho_0$  and  $\rho_1$  commute. Both relative entropies are monotone in the sense that

$$S(\rho_1, \rho_0) \geq S(E(\rho_1), E(\rho_0)), \quad S_{BS}(\rho_1, \rho_0) \geq S_{BS}(E(\rho_1), E(\rho_0))$$

holds for any subalgebra  $M_0$ . As we will see in the next section, equality in the monotonicity for  $S$  is equivalent with sufficiency of the subalgebra  $M_0$  with respect to  $\{\rho_0, \rho_1\}$ . For  $S_{SB}$ , we have the following result.

**Lemma 2** *The following are equivalent.*

$$(i) \ S_{BS}(\rho_1, \rho_0) = S_{BS}(E(\rho_1), E(\rho_0))$$

$$(ii) \ d_{\rho_0, \rho_1} \in N_{\rho_0}$$

$$(iii) \ \rho_1 \rho_0^{-1} \in M_0$$

$$(iv) \ \rho_1 \rho_0^{-1} = E(\rho_1)E(\rho_0)^{-1}$$

*Proof.* Since the function  $-\eta(x) = x \log(x)$  is operator convex,

$$\eta(d_{E(\rho_0), E(\rho_1)}) = \eta(E_{\rho_0}(d_{\rho_0, \rho_1})) \leq E_{\rho_0}(\eta(d_{\rho_0, \rho_1})) \quad (2)$$

by Jensen's inequality. We have

$$\text{Tr } \rho_0(E_{\rho_0}(\eta(d_{\rho_0, \rho_1})) - \eta(E_{\rho_0}(d_{\rho_0, \rho_1}))) = S_{BS}(\rho_1, \rho_0) - S_{BS}(E(\rho_1), E(\rho_0))$$

and since  $\rho_0$  is invertible, equality in the monotonicity of  $S_{BS}$  is equivalent with equality in (2). As it was proved in [14], this happens if and only if  $d_{\rho_0, \rho_1} \in N_{\rho_0}$ . This shows the equivalence (i)  $\leftrightarrow$  (ii). The equivalence of (ii) and (iii) follows by Lemma 1, (iii)  $\iff$  (iv) is rather obvious.  $\square$

## 2.3 Sufficient subalgebras

We say that the subalgebra  $M_0 \subseteq B(\mathcal{H})$  is sufficient for  $\{\rho_0, \rho_1\}$  if there is a completely positive trace preserving map  $T : M_0 \rightarrow B(\mathcal{H})$ , such that  $T \circ E(\rho_0) = \rho_0$  and  $T \circ E(\rho_1) = \rho_1$ . The following characterizations of sufficiency were obtained by Petz.

**Theorem 2** [10, 13] *The following are equivalent.*

$$(i) \ M_0 \subseteq B(\mathcal{H}) \text{ is sufficient for } \{\rho_0, \rho_1\}$$

$$(ii) \ S(\rho_1, \rho_0) = S(E(\rho_1), E(\rho_0))$$

$$(iii) \ \text{Tr } \rho_0^s \rho_1^{1-s} = \text{Tr } E(\rho_0)^s E(\rho_1)^{1-s} \text{ for some } s \in (0, 1)$$

$$(iv) \ \text{Tr } E_{\rho_0}(X) \rho_1 = \text{Tr } X \rho_1 \text{ for all } X \in B(\mathcal{H})$$

$$(v) \ E_{\rho_0} = E_{\rho_1}.$$

The next characterization is based on the Radon-Nikodym derivative.

**Theorem 3** *The subalgebra  $M_0 \subseteq B(\mathcal{H})$  is sufficient for  $\{\rho_0, \rho_1\}$  if and only if  $d_{\rho_0, \rho_1} \in F_{\rho_0}$ .*

*Proof.* Let us denote  $d = d_{\rho_0, \rho_1}$  and  $d_0 = d_{E(\rho_0), E(\rho_1)}$ . Since  $d_0 \in M_0$ , we have by definition that

$$\text{Tr } \rho_1 E_{\rho_0}(X) = \langle d_0, E_{\rho_0}(X) \rangle_{E(\rho_0)} = \langle d_0, X \rangle_{\rho_0}$$

so that  $\text{Tr } \rho_1 E_{\rho_0}(X) = \text{Tr } \rho_1 X$  if and only if  $\langle d_0, X \rangle_{\rho_0} = \langle d, X \rangle_{\rho_0}$ . It follows that  $d = d_0$  is equivalent with sufficiency of  $M_0$ , by Theorem 2 (iv). Since  $E_{\rho_0}(d) = d_0$ , this is equivalent with  $d_{\rho_0, \rho_1} \in F_{\rho_0}$ .  $\square$

### 3 Quantum hypothesis testing

Let us now turn to the problem of hypothesis testing. Any test of the hypothesis  $H_0 = \rho_0$  against the alternative  $H_1 = \rho_1$  is represented by an operator  $0 \leq M \leq 1$ , which corresponds to rejecting the hypothesis. Then we have the error probabilities

$$\begin{aligned} \alpha(M) &= \text{Tr } \rho_0 M && \text{first kind} \\ \beta(M) &= \text{Tr } \rho_1 (1 - M) && \text{second kind} \end{aligned}$$

For  $\lambda \in (0, 1)$ , we define the Bayes optimal test to be a minimizer of the expression

$$\lambda \alpha(M) + (1 - \lambda) \beta(M) \tag{3}$$

It is clear that minimizing (3) is the same as maximizing

$$\text{Tr } (\rho_1 - t\rho_0)M, \quad t = \frac{\lambda}{1 - \lambda}$$

#### 3.1 The quantum Neyman-Pearson lemma

The following is the quantum version of the Neyman-Pearson lemma. The obtained optimal tests are called the (quantum) Neyman-Pearson tests. We give a simple proof for completeness.

**Lemma 3** *Let  $t \geq 0$  and let us denote  $P_{t,+} := \text{supp } (\rho_1 - t\rho_0)_+$ ,  $P_{t,-} := \text{supp } (\rho_1 - t\rho_0)_-$  and  $P_{t,0} := 1 - P_{t,+} - P_{t,-}$ . Then the operator  $0 \leq M_t \leq 1$  is a Bayes optimal test of  $\rho_0$  against  $\rho_1$  if and only if*

$$M_t = P_{t,+} + X_t$$

where  $0 \leq X_t \leq P_{t,0}$ .

*Proof.* Let  $0 \leq M \leq 1$ , then

$$\begin{aligned} \text{Tr}(\rho_1 - t\rho_0)M &= \text{Tr}(\rho_1 - t\rho_0)_+M - \text{Tr}(\rho_1 - t\rho_0)_-M \leq \text{Tr}(\rho_1 - t\rho_0)_+M \\ &\leq \text{Tr}(\rho_1 - t\rho_0)_+ = \text{Tr}(\rho_1 - t\rho_0)P_{t,+} \end{aligned} \quad (4)$$

It follows that  $M_t = P_{t,+} + X_t$ ,  $X_t \leq P_{t,0}$  is a Bayes optimal test. Conversely, let  $M_t$  be some Bayes optimal test, then we must have

$$\text{Tr}(\rho_1 - t\rho_0)M_t = \text{Tr}(\rho_1 - t\rho_0)_+M_t = \text{Tr}(\rho_1 - t\rho_0)P_{t,+}$$

so that  $\text{Tr}(\rho_1 - t\rho_0)_-M_t = 0$ . By positivity, this implies that  $P_{t,-}M_t = M_tP_{t,-} = 0$ , so that

$$M_t(P_{t,+} + P_{t,0}) = (P_{t,+} + P_{t,0})M_t = M_t$$

which is equivalent with  $M_t \leq P_{t,+} + P_{t,0}$ . Furthermore, from

$$\text{Tr}(\rho_1 - t\rho_0)_+(P_{t,+} + P_{t,0} - M_t) = 0$$

we obtain  $P_{t,+} - P_{t,+}M_tP_{t,+} = P_{t,+}(1 - M_t)P_{t,+} = 0$ , hence  $(1 - M_t)P_{t,+} = 0$ . We obtain  $P_{t,+} \leq M_t$  and by putting  $X_t := M_t - P_{t,+}$ , we get the result.  $\square$

Let us denote by  $\Pi_{e,\lambda}$  the minimum Bayes error probability. Then

$$\begin{aligned} \Pi_{e,\lambda} &= \lambda\alpha(M_{\lambda/(1-\lambda)}) + (1-\lambda)\beta(M_{\lambda/(1-\lambda)}) = \\ &= \frac{1}{2}(1 - \|(1-\lambda)\rho_1 - \lambda\rho_0\|_1) \end{aligned} \quad (5)$$

where the last equality follows from

$$1 - t = \text{Tr}(\rho_1 - t\rho_0) = \text{Tr}(\rho_1 - t\rho_0)_+ - \text{Tr}(\rho_2 - t\rho_0)_-$$

and

$$\|\rho_1 - t\rho_0\|_1 = \text{Tr}|\rho_1 - t\rho_0| = \text{Tr}(\rho_1 - t\rho_0)_+ + \text{Tr}(\rho_2 - t\rho_0)_-$$

### 3.2 The quantum Chernoff bound

Suppose now that we have  $n$  copies of the states  $\rho_0$  and  $\rho_1$ , so that we test the hypothesis  $\rho_0^{\otimes n}$  against  $\rho_1^{\otimes n}$  by means of an operator  $0 \leq M_n \leq 1$ ,  $M_n \in \mathcal{B}(\mathcal{H}^{\otimes n})$ . Again, we may use the Neyman-Pearson lemma to find the minimum Bayes error probability

$$\Pi_{e,\lambda,n} = \frac{1}{2}(1 - \|(1-\lambda)\rho_1^{\otimes n} - \lambda\rho_0^{\otimes n}\|_1)$$



The following important result, obtained in [3] and [12] (see also [4]), is the quantum version of the classical Chernoff bound:

$$\lim_n \left( -\frac{1}{n} \log \Pi_{e,\lambda,n} \right) = -\log \left( \inf_{0 \leq s \leq 1} \text{Tr} \rho_0^{1-s} \rho_1^s \right) =: \xi_{QCB}(\rho_0, \rho_1) \quad (6)$$

The expression  $\xi_{QCB}$  has a number of interesting properties. For example, it was proved that it is always nonnegative and equal to 0 if and only if  $\rho_0 = \rho_1$ , moreover, it is monotone in the sense that

$$\xi_{QCB}(\rho_0, \rho_1) \geq \xi_{QCB}(E(\rho_0), E(\rho_1))$$

Therefore, although it is not symmetric,  $\xi_{QCB}$  provides a reasonable distance measure on density matrices, called the quantum Chernoff distance. Note also that in the case that the matrices are invertible, the infimum is always attained in some  $s^* \in [0, 1]$ .

## 4 2-sufficiency

We say that  $M_0$  is sufficient with respect to testing problems, or 2-sufficient, for  $\{\rho_0, \rho_1\}$  if for any test  $M$  and any  $\lambda \in (0, 1)$ , there is some test  $N_\lambda \in M_0$ , such that

$$\lambda \alpha(N_\lambda) + (1 - \lambda) \beta(N_\lambda) \leq \lambda \alpha(M) + (1 - \lambda) \beta(M)$$

It is quite clear that  $M_0$  is 2-sufficient if and only if for all  $t \geq 0$ , we can find a Neyman-Pearson test  $M_t \in M_0$ . Moreover, suppose that  $M_0$  is a sufficient subalgebra for  $\{\rho_0, \rho_1\}$  and let  $T = E_{\rho_0} = E_{\rho_1}$ . Then, if  $M_t$  is a Neyman-Pearson test, then  $T(M_t) \in M_0$  is a Neyman-Pearson test as well. Hence, a sufficient subalgebra is always 2-sufficient. In this section, we find the opposite implication in some special cases.

**Lemma 4**  *$P_{t,0} \neq 0$  if and only if  $t$  is an eigenvalue of  $d := d_{\rho_0, \rho_1}$ . Moreover, the rank of  $P_{t,0}$  is equal to multiplicity of  $t$ .*

*Proof.* By definition,

$$(\rho_1 - t\rho_0)P_{t,0} = \rho_0^{1/2}(d - t)\rho_0^{1/2}P_{t,0} = 0$$

so that  $(d - t)\rho_0^{1/2}P_{t,0}\rho_0^{1/2} = 0$ . Suppose  $P_{t,0} \neq 0$ , then  $t$  is an eigenvalue of  $d$  and any vector in the range of  $\rho_0^{1/2}P_{t,0}\rho_0^{1/2}$  is an eigenvector. This implies that  $r(P_{t,0}) = r(\rho_0^{1/2}P_{t,0}\rho_0^{1/2}) \leq r(F)$ , where  $F$  is the eigenprojection of  $t$ .

Conversely, let  $t$  be an eigenvalue of  $d$  with the eigenprojection  $F$ , then

$$(\rho_1 - t\rho_0)\rho_0^{-1/2}F\rho_0^{-1/2} = \rho_0^{1/2}(d - t)F\rho_0^{-1/2} = 0,$$

so that the range of  $\rho^{-1/2}F\rho^{-1/2}$  is in the kernel of  $\rho_1 - t\rho_0$ , this implies  $r(F) \leq r(P_{t,0})$ . □

Let us denote  $Q_{t,+} = \text{supp}(E(\rho_1) - tE(\rho_0))_+$ ,  $Q_{t,0} = \ker(E(\rho_1) - tE(\rho_0))$  and let  $\Pi_{e,\lambda}^0$  be the minimal Bayes error probability for the restricted densities

$$\Pi_{e,\lambda}^0 := \inf_{M \in M_0} \lambda\alpha(M) + (1 - \lambda)\beta(M) = \frac{1}{2}(1 - \|(1 - \lambda)E(\rho_1) - \lambda E(\rho_0)\|_1)$$

**Lemma 5** *The following are equivalent.*

- (i) *The subalgebra  $M_0$  is 2-sufficient for  $\{\rho_0, \rho_1\}$ .*
- (ii)  *$\Pi_{e,\lambda}^0 = \Pi_{e,\lambda}$  for all  $\lambda \in (0, 1)$ .*
- (iii)  *$Q_{t,0} = P_{t,0}$  and  $Q_{t,+} = P_{t,+}$  for all  $t \geq 0$ .*

*Proof.* It is obvious that (i) implies (ii). Suppose (ii) and let us denote  $f(t) := \max_{0 \leq M \leq 1} \text{Tr}(\rho_1 - t\rho_0)M$ . If  $N_t$  is any Neyman-Pearson test for  $\{E(\rho_0), E(\rho_1)\}$ , then

$$\text{Tr}(\rho_1 - t\rho_0)N_t = \text{Tr}(E(\rho_1) - tE(\rho_0))N_t = f(t),$$

so that  $N_t$  is a Neyman-Pearson test for  $\{\rho_0, \rho_1\}$  as well. Putting  $N_t = Q_{t,+}$  and  $N_t = Q_{t,+} + Q_{t,0}$ , we get by Lemma 3 that

$$Q_{t,+} = P_{t,+} + X_t, \quad Q_{t,+} + Q_{t,0} = P_{t,+} + Y_t,$$

with  $X_t, Y_t \leq P_{t,0}$ . This implies that  $Q_{t,0} \leq P_{t,0}$  and  $Q_{t,+} = P_{t,+}$  if  $P_{t,0} = 0$ .

Let  $t$  be an eigenvalue of  $d_0$ , then  $P_{t,0} \geq Q_{t,0} \neq 0$ , hence  $t$  is also an eigenvalue of  $d$ , and its multiplicity in  $d_0$  is not greater than its multiplicity in  $d$ . Since the sum of multiplicities must equal to  $m = \dim(\mathcal{H})$ , we must have  $r(Q_{t,0}) = r(P_{t,0})$ , so that  $Q_{t,0} = P_{t,0}$ . This implies that  $X_t \leq Q_{t,0}$ , hence  $X_t = 0$  and  $P_{t,+} = Q_{t,+}$  for all  $t$ .

The implication (iii)  $\rightarrow$  (i) is again obvious. □

Note that the condition (ii) is equivalent with

$$\|E(\rho_1) - tE(\rho_0)\|_1 \geq \|\rho_1 - t\rho_0\|_1, \quad \text{for all } t \geq 0$$

This condition, with  $E(\rho_0)$  and  $E(\rho_1)$  replaced by arbitrary densities  $\sigma_0$  and  $\sigma_1$  was studied in [2]. It was shown that for  $2 \times 2$  matrices, this is equivalent with the existence of a completely positive trace preserving map  $T$ , such that  $T(\rho_0) = \sigma_0$  and  $T(\rho_1) = \sigma_1$ . In our case, this means that 2-sufficiency implies sufficiency for  $2 \times 2$  matrices. Since any nontrivial subalgebra in  $\mathcal{M}(\mathbb{C}^2)$  is commutative, this agrees with our results below.

The above Lemma gives characterizations of 2-sufficiency, but the conditions are not easy to check. The next Theorem gives a simple necessary condition.

**Theorem 4** *Let  $M_0$  be 2-sufficient for  $\{\rho_1, \rho_0\}$ . Then  $d_{\rho_1, \rho_0} \in N_{\rho_0}$ .*

*Proof.* By the previous Lemma, we have  $P_{t,0} = Q_{t,0} \in M_0$  for all  $t$ . Let  $t_1, \dots, t_k$  be the eigenvalues of  $d$  and denote  $P_i = P_{t_i,0}$ . Then from  $(d - t_i)\rho_0^{1/2}P_i = 0$  we get

$$d\rho_0^{1/2} \sum_i P_i = \rho_0^{1/2} \sum_i t_i P_i$$

By Lemma 4 and its proof,  $\text{supp}(\rho_0^{1/2}P_i\rho_0^{1/2}) \leq F_i$  and  $r(P_i) = r(F_i)$ , with  $F_i$  the eigenprojection of  $t_i$ . It follows that  $\sum_i \rho_0^{1/2}P_i\rho_0^{1/2}$ , and hence also  $\sum_i P_i$ , is invertible. Therefore,

$$d\rho_0^{1/2} = \rho_0^{1/2}c, \quad c := \sum_i t_i P_i \left( \sum_j P_j \right)^{-1}$$

that is,  $d = \rho_0^{1/2}c\rho_0^{-1/2}$ , with  $c \in M_0$ . Moreover,  $d = d^* = \rho_0^{-1/2}c^*\rho_0^{1/2}$ , so that  $d \in \rho_0^{1/2}M_0\rho_0^{-1/2} \cap \rho_0^{-1/2}M_0\rho_0^{1/2}$ . By Lemma 1, this entails that  $d \in N_{\rho_0}$ .  $\square$

**Theorem 5** *Let the subalgebra  $M_0$  be 2-sufficient for  $\{\rho_0, \rho_1\}$ . Then  $M_0$  is sufficient for  $\{\rho_0, \rho_1\}$  in each of the following cases.*

- (1)  $\rho_0^{it}M_0\rho_0^{-it} \subseteq M_0$  for all  $t \in \mathbb{R}$
- (2)  $M_0$  is commutative
- (3)  $\rho_0$  and  $\rho_1$  commute

*Proof.* (1) By Theorem 4, we have  $d \in N_{\rho_0}$ . Since  $\rho_0^{it}M_0\rho_0^{-it} \subseteq M_0$ , we have  $d \in N_{\rho_0} = F_{\rho_0}$ . By Theorem 3, this implies that  $M_0$  is sufficient.

(2) Since  $d \in N_{\rho_0}$ , we have  $S_{BS}(\rho_1, \rho_0) = S_{BS}(E(\rho_1), E(\rho_0))$ , by Lemma 2. Since  $M_0$  is commutative,

$$S(E(\rho_1), E(\rho_0)) = S_{BS}(E(\rho_1), E(\rho_0)) = S_{BS}(\rho_1, \rho_0) \geq S(\rho_1, \rho_0)$$

By monotonicity of the relative entropy, this implies  $S(\rho_1, \rho_0) = S(E(\rho_1), E(\rho_0))$ , so that  $M_0$  is sufficient for  $\{\rho_0, \rho_1\}$ , by Theorem 2 (ii).

(3) Let  $M_1$  be the subalgebra generated by all  $P_{t,+}$ ,  $t \in \mathbb{R}$ . Then  $M_1$  is commutative and 2-sufficient for  $\{\rho_0, \rho_1\}$ , hence sufficient by (2). If  $M_0$  is 2-sufficient, we must have  $M_1 \subseteq M_0$  by Lemma 5, so that  $M_0$  must be sufficient for  $\{\rho_0, \rho_1\}$  as well.  $\square$

It is clear from the proof of (1) that 2-sufficiency implies sufficiency whenever  $N_{\rho_0} = F_{\rho_0}$  (or, equivalently,  $N_{\rho_1} = F_{\rho_1}$ ). In fact, it can be shown that  $N_{\rho_0} = F_{\rho_0}$  whenever  $M_0$  is commutative, which gives an alternative proof of (2). Next we give a further example of this situation.

**Example 1** Let  $\mathcal{H} = \mathbb{C}^4$  and let  $M_0 = \mathcal{M}(\mathbb{C}^2) \otimes I \subset B(\mathcal{H})$ . Let  $\rho$  be a block-diagonal density matrix  $\rho = \begin{pmatrix} \rho_1 & 0 \\ 0 & \rho_2 \end{pmatrix}$ , where  $\rho_1, \rho_2$  are positive invertible matrices in  $\mathcal{M}(\mathbb{C}^2)$ , and let  $\sigma$  be any density matrix. Suppose that  $M_0$  is 2-sufficient for  $\{\rho, \sigma\}$ .

By Theorem 4,  $d_{\sigma, \rho} \in N_\rho$ , which by Lemma 2 is equivalent with  $\sigma \rho^{-1} \in M_0$ . This implies that  $\sigma$  must be block-diagonal as well,  $\sigma = \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix}$ .

By Lemma 5,  $P_{t,+} \in M_0$  for all  $t \geq 0$ , so that  $P_{t,+} = \begin{pmatrix} p_t & 0 \\ 0 & p_t \end{pmatrix}$ , where  $p_t = \sup(\sigma_1 - t\rho_1)_+ = \sup(\sigma_2 - t\rho_2)_+$ . Since  $p_t$  is a projection in  $\mathcal{M}(\mathbb{C}^2)$ , we have the following two possibilities: either  $p_t = I$  for  $t < t_0$  and  $p_t = 0$  for  $t \geq t_0$ , or  $p_t$  is one-dimensional for  $t$  in some interval  $(t_0, t_1)$ . Since  $\rho = \sigma$  in the first case, we may suppose that the latter is true, so that  $p_t$  is a common eigenprojection of  $\sigma_1 - t\rho_1$  and  $\sigma_2 - t\rho_2$  for  $t \in (t_0, t_1)$ . It follows that  $\sigma_1 - t\rho_1$  commutes with  $\sigma_2 - t\rho_2$  for  $t \in (t_0, t_1)$ , which implies that  $\rho_1$  commutes with  $\rho_2$ .

Let  $X \in N_\rho$ , then  $X = \rho^{1/2} X_0 \rho^{-1/2}$ , where both  $X_0, \rho X_0 \rho^{-1} \in M_0$ . Let  $X_0 = Y \otimes I \in M_0$ , then  $\rho X_0 \rho^{-1} \in M_0$  if and only if  $\rho_1 Y \rho_1^{-1} = \rho_2 Y \rho_2^{-1}$ , that is,  $Y$  commutes with  $\rho_2^{-1} \rho_1$ . If  $\rho_2^{-1} \rho_1$  is a constant, then  $\rho^{it} M_0 \rho^{-it} \subseteq M_0$ , so that  $F_\rho = M_0 = N_\rho$ . Otherwise,  $Y$  must commute with both  $\rho_1$  and  $\rho_2$  and in this case,  $X = \rho^{1/2} X_0 \rho^{-1/2} = X_0 \in F_\rho$ .

In conclusion, if  $M_0$  is 2-sufficient for  $\{\rho, \sigma\}$ , we must have  $N_\rho = F_\rho$ , so that  $M_0$  must be a sufficient subalgebra.  $\square$

Let us now suppose that we have  $n$  independent copies of the states,  $\rho_0^{\otimes n}$  and  $\rho_1^{\otimes n}$ . An optimal test for  $H_1 : \rho_0^{\otimes n}$  against  $H_1 : \rho_1^{\otimes n}$  usually cannot be obtained as the product of optimal tests, but we may ask if there is some

optimal test in  $M_0^{\otimes n}$ . If this is the case for all  $\lambda$ , we say that  $M_0$  is  $(2, n)$ -sufficient for  $\{\rho_0, \rho_1\}$ .

**Theorem 6** *The following conditions are equivalent.*

- (i)  $M_0$  is  $(2, n)$ -sufficient for  $\{\rho_0, \rho_1\}$ , for all  $n$ .
- (ii)  $M_0$  is a sufficient subalgebra for  $\{\rho_0, \rho_1\}$ .

*Proof.* Let us denote

$$\Pi_{e,\lambda,n}^0 := \frac{1}{2}(1 - \|(1 - \lambda)E(\rho_1)^{\otimes n} - \lambda E(\rho_0)^{\otimes n}\|_1)$$

By Lemma 5 (ii), the condition (i) implies that  $\Pi_{e,\lambda,n} = \Pi_{e,\lambda,n}^0$  for all  $n$ , hence also

$$\lim_n \left(-\frac{1}{n} \log \Pi_{e,\lambda,n}\right) = \lim_n \left(-\frac{1}{n} \log \Pi_{e,\lambda,n}^0\right)$$

By (6), this entails that

$$\inf_{0 \leq s \leq 1} \text{Tr } \rho_0^{1-s} \rho_1^s = \inf_{0 \leq s \leq 1} \text{Tr } E(\rho_0)^{1-s} E(\rho_1)^s$$

By monotonicity, we have  $\text{Tr } \rho_0^{1-s} \rho_1^s \leq \text{Tr } E(\rho_0)^{1-s} E(\rho_1)^s$  for all  $s \in [0, 1]$ . Suppose that the infimum on the RHS is attained in some  $s_0 \in [0, 1]$ . Then

$$\text{Tr } E(\rho_0)^{1-s_0} E(\rho_1)^{s_0} = \inf_{0 \leq s \leq 1} \text{Tr } \rho_0^{1-s} \rho_1^s \leq \text{Tr } \rho_0^{1-s_0} \rho_1^{s_0}.$$

If  $s_0 = 0$  or  $1$ , then the quantum Chernoff distance is equal to  $0$ , so that  $\rho_0 = \rho_1$  and the subalgebra  $M_0$  is trivially sufficient. Otherwise, we must have  $\text{Tr } E(\rho_0)^{1-s_0} E(\rho_1)^{s_0} = \text{Tr } \rho_0^{1-s_0} \rho_1^{s_0}$  for  $s_0 \in (0, 1)$ , which implies that  $M_0$  is sufficient for  $\{\rho_0, \rho_1\}$ , by Theorem 2 (iii).

Conversely, let  $E_{\rho^{\otimes n}}$  be the generalized conditional expectation  $B(\mathcal{H}^{\otimes n}) \rightarrow M_0^{\otimes n}$ . It is easy to see that for any invertible density matrix  $\rho$ ,  $E_{\rho^{\otimes n}} = E_\rho^{\otimes n}$ , so that if  $E_{\rho_0} = E_{\rho_1}$ , then  $E_{\rho_0^{\otimes n}} = E_{\rho_1^{\otimes n}}$  for all  $n$ . Hence if  $M_0$  is sufficient for  $\{\rho_0, \rho_1\}$ , then  $M_0^{\otimes n}$  is sufficient for  $\{\rho_0^{\otimes n}, \rho_1^{\otimes n}\}$  for all  $n$ , this implies (i).  $\square$

## References

- [1] L. Accardi, C. Cecchini, Conditional expectations in von Neumann algebras and a theorem of Takesaki, J. Functional. Anal. **45**(1982), 245–273.

- [2] P. M. Alberti, A. Uhlmann, A problem relating to the positive linear maps on a matrix algebra, Rep. Math. Phys. **18** (1980), 163–176
- [3] K.M.R. Audenaert, J. Calsamiglia, L. Masanes, R. Muñoz-Tapia, A. Acín, E. Bagan, F. Verstraete, Discriminating states: The quantum Chernoff bound, Phys. Rev. Lett. **98**, 160501 (2007)
- [4] K.M.R. Audenaert, M. Nussbaum, A. Szkola, F. Verstraete, Asymptotic error rates in quantum hypothesis testing, Comm. Math. Phys. **279**, 251–283 (2008)
- [5] V.P. Belavkin, P. Staszewski,  $C^*$ - algebraic generalizations of relative entropy and entropy, Ann. Ins. Henri Poincaré Sec. A **73** (1982), 51–58
- [6] C.W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, 1976
- [7] F. Hiai, D. Petz, The proper formula for relative entropy and its asymptotics in quantum probability, Comm. Math. Phys. **143** (1991), 99–114
- [8] A.S. Holevo, On asymptotically optimal hypothesis testing in quantum statistics, Theor. Prob. Appl. **23** (1978), 411–415
- [9] A. Jenčová, D. Petz, Sufficiency in quantum statistical inference. Commun. Math. Phys. **263**, 259276 (2006).
- [10] A. Jenčová, D. Petz, Sufficiency in quantum statistical inference. A survey with examples, IDAQP 9 (2006), 331–351
- [11] E.H. Lieb, M.B. Ruskai, Some operator inequalities of the Schwarz type, Adv. Math. **12** (1974), 269–273
- [12] M. Nussbaum, A. Szkola, The Chernoff lower bound for symmetric quantum hypothesis testing, Annals of Statistics **37**, No. 2, 1040–1057 (2009)
- [13] M. Ohya, D. Petz, *Quantum Entropy and Its Use*, Springer-Verlag, Heidelberg, 1993, 2nd edition 2004.
- [14] D. Petz, On the equality in Jensen’s inequality for operator convex functions, Integral Equations and Operator Theory, **9** (1986), 744–747
- [15] J. Pfanzagl, A characterization of sufficiency by power functions, Metrika **21** (1974), 197–199
- [16] H. Strasser, *Mathematical theory of statistics. Statistical experiments and asymptotic decision theory*, Walter de Gruyter, Berlin, 1985.